Act and Actor Attribution in Cyberspace

A Proposed Analytic Framework

Eric F. Mejia, Colonel, USAF

TSgt Joe Pesek rolled out of bed shortly after 0600 to get breakfast at the NCO club. He was assigned to the 5th Bomber Group and had arranged to meet his friends for golf after breakfast. The course in Honolulu was beautiful, and there was no better way to spend a lazy Sunday morning. Waiting for the bus, he admired the beautiful blue sky flecked with distant aircraft. Seeing this many aircraft meant a carrier must be coming into port. Joe wasn't alarmed until the first plane pulled up low over Hickam Airfield with machine guns chattering. The clearly visible rising sun of Imperial Japan on the wings told the story—Japan had attacked Pearl Harbor.[1] The following day, 8 December 1941, the United States and Japan declared war against each other.

Seventy years later, Air Force major Shelly Johnson rolled out of bed looking forward to another day of leave in Honolulu. Taking out her smartphone, she tried to scan a check into her account so she would have extra spending money. Despite several attempts, the check failed to deposit. Frustrated, she used her tablet to access the bank's website; however, the homepage refused to load. She finished breakfast and tried again without luck. Irritated, she gave up and got into her car to enjoy her day of leave. A few days later she read the headline: "Major Banks Hit with Biggest Cyberattacks in History."[2] The article explained how several of the largest banks, including her own, had been the victim of a cyber attack. The Islamist group Izz ad-Din al-Qassam Cyber Fighters claimed responsibility for the attacks; however, researchers were divided about whether they were responsible. Senator Joe Lieberman claimed the attacks were actually conducted by Iran in response to US economic sanctions. The article provided more questions than answers. Major

---

Col Eric F. Mejia, USAF (JAG) is currently assigned as staff judge advocate at Eglin AFB. He holds a JD degree from the University of Arkansas at Little Rock Law School, is a 2004 distinguished graduate of the Air Command and Staff College, and graduated from the Air War College in 2013, receiving his Master of Strategic Studies degree with highest academic distinction.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Strategic Studies Quarterly (SSQ),155 N. Twining Street, Building 693,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**19**	

Johnson wondered who actually conducted the attack. Could it even be considered an attack, and if so, what was attacked: the customers, the individual banks, the US economy? Who would respond, and how?

These two scenarios highlight the critical importance of attribution. In the case of Pearl Harbor, there was a hostile armed attack directly attributable to a known state actor. These facts established the proper response—war—and the proper responder: the military. In the second scenario, the act and actor were uncertain; consequently, the proper response and responder were equally uncertain. *Actor attribution* is concerned with determining who is responsible for a hostile cyber act. *Act attribution* is concerned with the relative severity of the act. Both are necessary to determine the appropriate response to an act of cyber hostility, and both help frame which organization should be the primary responder. An analytic framework incorporating both act and actor attribution helps delineate responsibility for hostile cyber acts and determine the appropriate response. This article examines the definition and importance of cyber attribution and proposes such an analytic framework for considering act and actor attribution. It concludes with recommendations to address the problems associated with such attribution.

Defining Attribution

The Basic Legal Framework

It is clear, at least from the US perspective, that cyberspace is not a "law-free" zone and that established principles of international law apply.[3] The legal framework for use of force by states is contained in the *Charter of the United Nations*, which generally prohibits states from using force against another state. As specified in Article 2(4), "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[4] The charter recognizes two exceptions. First, Article 42 permits use of force if authorized by the UN Security Council. Second, and more important for our analysis, Article 51 permits use of force in self-defense against an armed attack, stating that "nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."[5] These

articles did not originally apply to the conduct of nonstate actors. However, international law has developed so that states may use force in self-defense against another state for acts of nonstate actors attributed to it.[6] A state may also use defensive force directly against nonstate actors if the host state is unable or unwilling to prevent armed attacks from emanating within its territory.[7]

Finally, the use of force is bounded by the law of armed conflict (LOAC), including the concepts of distinction, necessity, and proportionality. Applying the LOAC to hostile cyber acts may cause unnecessary concern among lawyers and unnecessary hesitancy among commanders. This is because responding to a hostile cyber act will likely involve targeting dual-use objects and because of the perceived increased risk of "knock-on," or unexpected collateral damage.

Dual-use objects may serve both a military and civilian function. The typical example is a bridge, which is equally useful for conveying both military and civilian vehicles. Similarly, most hostile cyber acts will transit civilian cyber infrastructure, including computing systems, data storage systems, and telecommunication lines. Further, malicious cyber code may be prepositioned on civilian cyber infrastructure. Despite the fact that these are clearly dual-use objects, the LOAC often permits them to be targeted. Addressing the issue involves applying Article 52(2) of the Protocol additional to the Geneva Conventions (GPI) to the facts.[8] Although the United States has not ratified the GPI, it recognizes Article 52(2) as binding customary international law. Article 52(2) sets out a two-part test for analyzing whether an object is an appropriate military target. The first issue is one of *distinction*—is the object a legitimate military objective? Article 52(2) limits attacks to objects who's "nature, location, purpose or use make an effective contribution to military action." In the case of hostile cyber acts, cyber infrastructure may be a legitimate military objective if it is used to conduct a hostile cyber act or if malicious code is prepositioned on it in anticipation of a future hostile use. In either case, the use of the object may make it a legitimate military objective and therefore appropriately targetable. The second issue is one of *necessity*. Does the total or partial destruction or neutralization of the object, in the circumstances ruling at the time, offer a definite military advantage? In the case of an ongoing hostile cyber act or prepositioned malicious code, this is a fairly low hurdle to overcome, especially after

making the initial determination that the object is a legitimate military objective.

The potential for unexpected collateral damage is another issue that appears difficult at first blush. Although the facts may be more complicated, traditional application of LOAC is all that is required. Here, the issue is one of proportionality—an attack is generally prohibited if the damage to noncombatants is excessive in relation to the military advantage gained from the attack. The problem with attacking dual-use cyber infrastructure is that it is difficult, if not impossible, to fully anticipate the extent of the likely collateral damage. Luckily, that is not required. In attempting to predict collateral damage, the commander is "only required to do what is feasible, given the prevailing circumstances, including the time he has to make a decision and the amount of information he has at that time."[9] If anything, the difficulty of precisely determining what collateral damage may be expected benefits commanders by affording them significant latitude in the decision-making process.

The basic legal framework may be summarized as follows:

- States may generally not use force against other states.
- States may use force against other states if
  a. force is authorized by the UN Security Council, or
  b. force is used in self-defense against an armed attack by (1) another state or (2) a nonstate actor if the act can be imputed to a state.
- Force may be used in self-defense directly against nonstate actors if the host state is unable to prevent armed attacks by nonstate actors.
- Use of force is limited by LOAC principles.

Ultimately, determining an appropriate response to a hostile cyber act requires analyzing who the actor is (state, nonstate, unknown) and what the act is (armed attack or not an armed attack). In other words, actor and act attribution.

Actor Attribution

Actor attribution is simply determining who should be held responsible for a hostile cyber act. As noted in the *2011 Department of Defense Strategy for Operating in Cyberspace*, low barriers to entry for hostile cyber acts, coupled with widespread availably of hacking tools, means

that small groups, and even individuals, can impact national security.[10] However, a significant issue from a response perspective is not the identity of the actors but whether the hostile cyber acts are attributable to a specific state. This distinction helps determine the appropriate response, responder, and rules for engagement.

Hostile cyber acts can be attributed to a state either directly or indirectly.[11] The two methods of state attribution are briefly described as follows:

> **Direct Attribution**. States are responsible for the acts or omissions of individuals exercising the state's machinery of power and authority since these actions are attributed to the state even if the acts exceed the authority granted by the state.
>
> **Indirect Attribution**. Acts or omissions of nonstate actors are generally not attributable to the state; however, the state may incur responsibility if it fails to exercise due diligence in preventing or reacting to such acts or omissions.[12]

Although not universally accepted in international law, it is generally accepted in practice that a state's right to use force in self-defense is also triggered by armed attacks which cannot be attributed to a state. For example, an armed attack may emanate from a state without that state's knowledge or ability to prevent it. In such circumstances, the armed attack is attributed directly to the attackers, and the victim state may defend with force directly against the nonstate actors despite their being located in a neutral or even allied state. As recently noted in the *Journal of Conflict and Security Law*, it is the nature of the hostile act that triggers the right to self-defense, not the nature of the actor.[13] This simply comports with common sense. A state should not be required to endure an armed attack by nonstate actors when it has the means to defend itself consistent with fundamental LOAC principles. US attacks against terrorists operating within Pakistan are one concrete application of this concept. Once a state has been subjected to an armed attack, it may forcibly defend itself. The decision of whether to do so is a matter of policy, and ultimately the response must satisfy basic LOAC principles including necessity, proportionality, and distinction.

Act Attribution

Act attribution is the process of defining the severity of the hostile cyber act.[14] Hostile cyber acts may range from something as benign as attempting to ping a network computer to an attack on the US power grid leaving millions without power for months.[15] Similarly, there is a broad range of potential defensive actions that may be taken by the victim state. A simple continuum of potential responses is presented in figure 1.

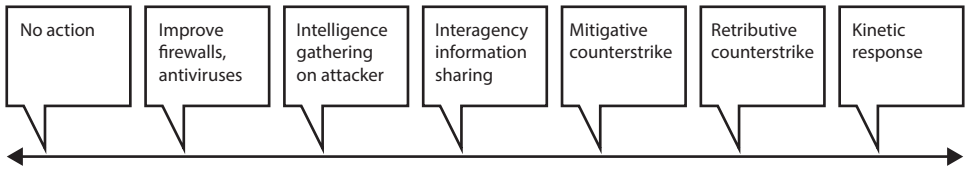

Figure 1. Continuum of potential cyber-attack responses

Supplementing these potential actions is a state's full range of diplomatic and political responses to cyber hostility. However, any response by a victim state must be determined in part by the severity of the hostile act.

A state may passively defend against all hostile actions; however, it may only forcibly retaliate in self-defense against armed attacks. By extension, imminent armed attacks allow states to respond in anticipatory self-defense.[16] International law currently is silent on whether a cyber attack can be considered an armed attack. However, the United States has taken an affirmative position on the issue. The May 2011 *International Strategy for Cyberspace* states, "Right of Self-Defense: Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."[17] This echoes the language of Article 51 of the UN charter which says that states have the inherent right to engage in individual or collective self-defense in response to an armed attack.[18] So, clearly the United States has adopted the position that a hostile cyber act may be treated as an armed attack. But given the range of hostile cyber actions, how do we determine whether such an act rises to the level of an armed attack? If the *effects* of a cyber attack are the equivalent of a traditional armed attack, then states should be permitted to respond accordingly. The leading proponent of this effects-based approach is Michael N. Schmitt. His effects-based analysis evaluates hostile cyber acts based on six criteria:

1. Severity: Armed attacks threaten physical injury or destruction of property to a greater degree than other forms of coercion.
2. Immediacy: Armed attacks usually occur with greater immediacy.
3. Directness: Armed attacks have a more direct link to the negative consequences caused.
4. Invasiveness: Armed attacks usually cross into the target state to cause harm.
5. Measurability: The consequences of an armed attack are easier to measure.
6. Presumptive Legitimacy: Because of the general prohibition on the use of armed force between states in international law, an armed attack is presumed illegitimate.[19]

This framework can readily be applied to cyber attacks to determine whether a given hostile act may be considered an armed attack.[20] If so, a forcible response may be appropriate. If not, some lesser form of response may be required.

The Importance of Attribution

An assessment of both act and actor attribution is central in determining the appropriate response to a hostile cyber act. A government may respond in a variety of ways including monitoring, improving passive defenses, applying political pressure, employing active defenses, and counterstriking with both cyber and conventional weapons. *Passive defense* is defined as "measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative."[21] Passive defense in the cyber realm includes making systems more difficult to attack through antiviruses and firewalls, educating users to be more security conscious, and reducing postattack recovery times through redundancy and backup systems.[22] By contrast, *active defense* is "the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."[23] In the cyber realm this translates to initiating a cyber counterattack as a defensive response to a hostile cyber attack.[24] Defensive cyber attacks can be broken down into two types. If the goal is to mitigate harm to a targeted system using only the amount of force necessary to protect the

system from further damage, it is considered a mitigative counterstrike. The purpose of a mitigative counterstrike must be to mitigate damage from an immediate threat. If the goal of the counterstrike is to punish the attacker, it is considered a retributive counterstrike.[25] Under international law, only the mitigative counterstrike is truly defensive, because its purpose is to defend against an immediate threat.

Actor and act attribution is also critical in determining which government entity should take the lead in responding to a hostile cyber act. Several government agencies are tasked with cyber operations and responsibilities. As summarized by Gen Keith B. Alexander, commander for US Cyber Command (CYBERCOM), these agencies include:

- Department of Defense/Intelligence Community/NSA/CYBERCOM: Responsible for detection, prevention, and defense in foreign space, foreign cyber threat intelligence and attribution, security of national security and military systems, and, in extremis, defense of the homeland if the nation comes under cyber attack from a full scope actor.
- Department of Homeland Security (DHS): Lead for coordinating the overall national effort to enhance the cyber security of US critical infrastructure and ensuring protection of the civilian federal government (.gov) networks and systems.
- Federal Bureau of Investigation (FBI): Responsible for detection, investigation, prevention, and response within the domestic arena under their authorities for law enforcement, domestic intelligence, counterintelligence, and counterterrorism. Importantly, when malicious cyber activity is detected in domestic space, the FBI takes the lead to prevent, investigate, and mitigate it.[26]

The Difficulty of Conclusive Attribution

Both act and actor attribution are difficult to prove with scientific certainty. Computer networks are not designed to facilitate attribution, and hostile actors exploit this weakness to hide their true identity. For example, the Internet typically does not use sender identification during the transmission process, so source information can easily be forged. Masking the sender information in this manner is commonly referred to as "spoofing." Hostile cyber actors can also hide their identity and

location by employing a system that transforms data in some manner, known as a "laundering host." Cyber actors may employ an attack that is complete in milliseconds, or alternatively, is spread out over months. All of these factors make cyber actor attribution difficult.[27] The degree of difficulty is subject to some debate. Former secretary of defense Leon Panetta stated in late 2012 that the Department of Defense had made "significant investments in forensics to address this problem of attribution" and that "potential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America."[28] However, such a public declaration raises several issues. First, is the statement an accurate assessment of capabilities or is it more akin to posturing in an attempt to deter potential adversaries? Second, if the statement is technologically accurate, acknowledging this capability and subsequently using it to attribute a hostile act to a specific actor runs the risk of compromising the methods and techniques used in the process. Finally—given the highly adaptive nature of cyber warfare—cyber defenses, including forensics, will inevitably be thwarted by constantly evolving cyber threats. Even if the technical issue of attribution is overcome, what degree of confidence must be achieved to support a finding that a state is responsible under international law? Certain? Very certain? These are subjective political determinations that simply do not lend themselves to precise quantitative analysis.

This same issue exists when trying to assess act attribution. Using the Schmitt model to determine if a hostile cyber act is tantamount to an armed attack requires applying a subjective analysis. How severe is *severe*? What is the definition of *immediate*? What constitutes a *direct link* between a hostile cyber act and the consequences of the act? All of these questions require a subjective, nonscientific assessment.

Fortunately, the legal community has been dealing with the problem of subjective actor and act attribution and has extensively developed the concepts and lexicon related to subjective attribution. This is most evident in the law related to civil and criminal trials. Legal experts refer to these subjective criteria as "standards of proof." A few of the more common ones, in order of the degree of certainty, are:

- Scintilla of evidence—the least amount of evidence possible.

- Preponderance of the evidence—In a civil trial the issue to be decided is often whether or not one party is negligent, and therefore financially responsible for the losses incurred by the other party. The subjective standard used by courts to assess this question of liability is called the preponderance of the evidence standard. This is simply defined as more probable than not.
- Clear and convincing evidence—creating a firm belief or conviction. It is an intermediate level of proof, being more than a preponderance of the evidence but less than what is required for proof beyond a reasonable doubt.
- Beyond a reasonable doubt—This is the standard used to establish criminal guilt, which is the equivalent of actor attribution, as well as to determine the specific criminal offense committed, which is the equivalent of act attribution. It means entirely convinced and satisfied to a moral certainty. However, it is less than a scientific certainty.[29]

Employing legal subjective criteria is not a new or novel idea. In a 2009 Microsoft white paper, the author suggested a similar subjective assessment for cyber attribution, noting that

> it [is] important to focus on probability of accurate attribution, as opposed to certainty of attribution. In many areas, of course, absolute certainty is seldom achievable. For this reason, a range of different standards have developed (for example, proof beyond a reasonable doubt, a preponderance of the evidence) and individuals and organizations often have to rely upon probabilities when making critical decisions (such as when opting for one medical treatment over another). Of course, the greater the certainty, the easier it may be to choose a course of action, but that does not mean certainty is required before reasonable action can be taken.[30]

While it would be naïve to assume that one could import the whole of court-based attribution concepts to assess cyber attribution, several key points are evident. First, scientific proof is not necessary for attribution. While scientific certainty is the "gold standard" of proof, it is rarely obtainable, and historically has not been necessary to establish attribution. Second, as previously noted, attribution is routinely based on subjective determinations. Third, when using a subjective assessment of attribution, severity of the consequences is linked to the degree of confidence. A court may assess financial responsibility based on a preponderance of the evidence, but it takes a much higher degree of confidence to establish

criminal guilt. Finally, although many technical experts may be hesitant or uncomfortable using a subjective assessment, the government, through its legal community, has at its disposal established expertise in subjective attribution.

An Analytic Model for Actor and Act Attribution

Based on the foregoing, the factors included in any proposed analytic model should be based on a subjective assessment of act and actor attribution. An assessment of these factors should indicate who should respond to an act of cyber hostility and what the upper range of appropriate responses should be. Ideally, the responses would incorporate basic LOAC principles. Combining these basic concepts yields the analytic model proposed in figure 2.

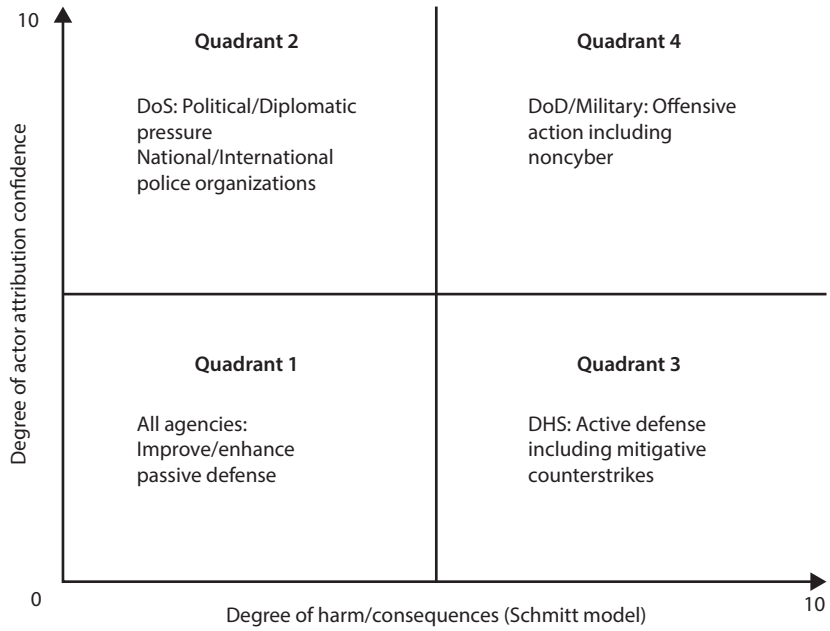

Figure 2. Analytic model for actor and act attribution

Several issues are worth noting. First, act and actor attribution are dynamic. Just as in conventional warfare, the preparation for a hostile cyber act may occur in one location, yet the act itself may originate in a different location or, even more likely, be distributed throughout a variety of locations. Further, although an act may appear harmless at first,

subsequent information or events may show it to be significantly more harmful than initially believed. Therefore, the appropriate response and responder are likely to be dynamic as well, involving several organizations and a potentially escalating series of responses. Second, the responsive actions in each quadrant represent the upper limits of an appropriate response. For example, the Department of State (DoS) may elect not to apply diplomatic pressure to a state actor for a variety of reasons, even if justified by hostile cyber acts. Further, the various instruments of power described are not equally effective on all hostile actors. For example, it is unlikely that a rouge individual would be greatly deterred by political/diplomatic pressure. Although a military strike against an individual would likely be effective, it is politically untenable. As always, effective application of the instruments of power is an art, and a mechanistic approach will likely fail. Finally, the quadrants do not reflect sole responsibility for responding to hostile cyber acts. However, the framework does help assign primary or lead responsibility, with other agencies in a supporting role.

Quadrant 1: Low Actor Attribution Confidence/Low Degree of Harm

In this common scenario, government agencies are faced with numerous relatively innocuous yet unauthorized cyber acts. For example, in 3 June 2010, General Alexander stated that DoD systems are probed by unauthorized cyber actors approximately 250,000 times per hour, or the equivalent of more than 6 million times each day.[31] Most cause no damage and do not result in a compromise of data. According to the US Computer Emergency Readiness Team (US-CERT), in 2009, approximately 73.4 percent of all reported cyber incidents were categorized as "Category 5: Scans, Probes, or Attempted Access." This includes "any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service."[32] For these types of acts, passive defense is an appropriate response. The vast majority of Quadrant 1 actions are easily defeated by encryption, firewalls, antivirus and anti-malware programs, or other purely passive measures.

Quadrant 2: High Actor Attribution Confidence/Low Degree of Harm

In this scenario, the government is again faced with acts that cause little harm. However, the acts are still unauthorized and may be the harbinger of more serious, and more harmful, future acts. Unlike the scenario in Quadrant 1, these acts can confidently be attributed to an identified actor. Under these circumstances, passive defensive measures alone may be insufficient. However, because the acts are insufficiently harmful to be considered equivalent to an armed attack, offensive strikes and defensive counterstrikes are not necessary or proportional to the harm being caused. In addition to passive defense, employing appropriate diplomatic pressure may be appropriate for state actors. This approach is consistent with the May 2011 *International Strategy for Cyberspace*. This document states that the United States will combine diplomacy, defense, and development to achieve the national goal of cyber security. Diplomatic efforts will be focused on engaging "the international community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace and the actions necessary, both domestically and as an international community, to build a system of cyberspace stability."[33] Diplomatic efforts to stem the tide of less serious cyber acts are not new. For several years the United States has been engaged in such efforts to dissuade China from continuing cyber espionage against both the US government and US corporations. Former defense secretary Leon Panetta spent three days in China addressing the issue of its cyber activity. This is an appropriate response to state-attributed cyber acts which fall short of an armed attack. As noted by James Lewis, cyber security expert with the Center for Strategic and International Studies, "The damage from Chinese cyber espionage is easy to overstate but that doesn't mean we should accept it."[34] To facilitate diplomatic efforts at cyber security, the DoS recently created a new office. The Office of the Coordinator for Cyber Issues is tasked with coordinating DoS global diplomatic engagement on cyber issues, serving as the DoS liaison to the White House and federal departments and agencies on cyber issues, and advising the secretary and deputy secretaries on cyber issues and engagements.[35] If the hostile actor is a non-state-affiliated individual or group, the Federal Bureau of Investigation, Department of Justice, or analogous international organizations will be primarily responsible for any investigation and prosecution, if appropriate.

Quadrant 3: Low Actor Attribution Confidence/High Degree of Harm

In this scenario, the government is faced with a hostile cyber act capable of causing significant harm. The harm threatened, or caused, may be sufficient to be considered the equivalent of an armed attack. Within the cyber realm, this may involve harming the nation's key resources or critical infrastructure. However, there is insufficient evidence to confidently attribute the act to a specific state or nonstate actor. One potential example of this would be unidentified actors using a state's IT infrastructure to conduct an attack without the consent, or even knowledge, of that state. Retributive strikes require attribution, which is lacking in this scenario. However, the LOAC still permits action in self-defense. When a state is unable to prevent attacks emanating from inside its borders or the attackers operate independently of the state, the victim state may still use force in self-defense, provided it meets the requirements of necessity, proportionality, and distinction.[36] Under these circumstances, active defenses, including mitigative counterstrikes, may be appropriate. The goal of mitigative counterstriking is to "mitigate damage from a current and immediate threat."[37] These active but purely defensive measures can trace an attack back to its source and immediately interrupt the attack. Further, mitigative counterstrikes are relatively precise. This precision limits the risk of excessive collateral damage. Limiting collateral damage helps satisfy the requirement of proportionality and helps reduce the risk of escalating cyber attacks into full-scale kinetic attacks between states.[38] Finally, because of their precision, reduced risk of collateral damage, and purely defensive nature, automated mitigative counterstrikes are less likely to violate international LOAC norms.

Mitigation of cyber attacks is squarely within the purview of the DHS. *Homeland Security Presidential Directive 7* establishes the national policy for identifying and protecting critical US infrastructure and defines the roles of the various federal and state departments. The secretary of homeland security is responsible for "coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States [and serves as] the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources."[39] To fulfill this responsibility, DHS created the National Cyber Security Division,

which is responsible for analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems.[40] One of its specified missions is safeguarding and securing cyberspace, and one of its key strategic outcomes in performing this mission is that "cyber disruptions or attacks are detected in real-time [*sic*], consequences are mitigated, and services are restored rapidly."[41]

Quadrant 4: High Actor Attribution Confidence/High Degree of Harm

In this scenario, the government is faced with a hostile cyber act tantamount to an armed attack. Further, there is a high degree of actor attribution confidence. Conceptually, this is the equivalent of a kinetic attack against the United States, therefore a DoD response is appropriate. Further, there is no prohibition against responding with kinetic force against a cyber attack provided the response meets traditional LOAC requirements. This, too, is consistent with the 2011 *International Strategy for Cyberspace*, which states: "We fully recognize that cyberspace activities can have effects extending beyond networks; such events may require responses in self-defense. . . . When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country."[42]

There is little disagreement that the DoD should be the lead agency in this scenario. As noted by the US CYBERCOM commander, in extreme situations, it is the role of the DoD to defend "the homeland if the Nation comes under cyber attack from a full scope actor."[43] However, some argue that the DoD should take a more expansive role in cybersecurity, essentially performing the DHS's assigned role. Much of this argument is based on the perceived effectiveness of the DoD, or rather the perceived ineffectiveness of the DHS. However, an expanded role for the DoD in cybersecurity is the wrong approach. First, it unnecessarily expands the role of the military. The military would undoubtedly perform well at securing transportation hubs, power plants, water treatment facilities, critical manufacturing sites, and other critical national infrastructure. However, that is not the mission of the military; the mission of the military is to wage war. Further, effective cyber defense requires a degree of domestic intrusion which should not be conducted by the DoD. As noted by retired major general Charles Dunlap, "The armed

forces are the most authoritarian, least democratic, and most powerful institution in American society. The restraint intrinsic to a domestic law enforcement mind-set is not its natural state. . . . If nothing else, the fact that the armed forces unapologetically restrict the rights and privileges of their own members should militate toward avoiding their use in civilian settings where the public properly expects those rights and privileges to flourish."[44]

Conclusion and Recommendations

The cyber community must recognize the critical importance of attribution. It is the basis for effective diplomacy, law enforcement, and a prerequisite for offensive military counterstrikes under the law of armed conflict. The first fundamental question that must be answered after a hostile act is: who committed the act? The second is: how much damage was done? An accurate assessment of actor and act attribution helps define both the proper response to an act of cyber aggression and helps determine the appropriate lead agency to respond to such an act.

Because actor and act attribution fundamentally drive cyber defense, efforts to enhance technical attribution should be given priority. Although assessing attribution is subjective, often the evidence used in such an assessment is technical. Attributing a hostile cyber act is a prerequisite to effective deterrence. No hostile actor, whether nation-state or rogue individual, will ever be deterred from hostile cyber activity if they can effectively deny responsibility. Further, the international community is unlikely to support military action unless a hostile act equivalent to an armed attack can successfully be attributed to an offending party. Because hostile actors will continue to develop new methods to mask their activity, effective deterrence demands that the United States continue to enhance its technical attribution capability.

Legal expertise is critical in assessing attribution and framing an appropriate response. Although the cyber domain is relatively new, the art of actor and act attribution is ancient. Every criminal prosecution that has ever occurred fundamentally required a subjective determination of guilt (actor attribution) and offense (act attribution). Legal practitioners, although often ignorant of the technical aspects of the cyber domain, are well versed in the art of attribution. Cyber experts may be technically adept but are often ignorant of the nuances of subjective

attribution. Close integration of both legal experts and technical cyber experts is critical to establishing an appropriate cyber policy and appropriate responses to specific hostile cyber acts.

An analytic framework is an essential tool for cyber practitioners. In a field where significant ambiguity may exist, both as to the nature of the act and the identity of the actor, an analytic construct promotes diagnostic consistency. Additionally, it helps define roles and missions for various responders and provides a common framework and understanding of responsibility. The analytic framework also enhances deterrence by providing notice to hostile cyber actors that the consequences they should expect from committing a hostile cyber act are determined, in part, by the severity of the hostile act and that a severe hostile act will merit a military response. SSQ

Notes

1. "Hickam Field—Army Air Corp Sergeant," *PearlHarbor.org,* http://www.pearlharbor.org/eyewitness-accounts.asp.
2. David Goldman, "Major Banks Hit with Biggest Cyber Attacks in History," *CNN.com*, 28 September 2012, http://money.cnn.com/2012/09/27/technology/bank-cyberattacks /index.html.
3. Harold Hongju Koh, Department of State legal advisor, "International Law in Cyberspace," remarks to the USCYBERCOM Interagency Legal Conference, Ft. Meade, MD, 18 September 2012, http://www.state.gov/s/l/releases/remarks/197924.htm.
4. *Charter of the United Nations*, 24 October 1945, chap. I, art. 2(4).
5. Ibid., chap. VII, art. 51.
6. Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2012), 53.
7. Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (Summer 2012): 7, http://jcsl.oxfordjournals.org/content/17/2/229.full.pdf+html.
8. "Protocol additional to the Geneva Conventions of 12 August 1949 and relating to the protection of victims of international armed conflicts (Protocol I)," adopted at Geneva on 8 June 1977, http://treaties.un.org/doc/Publication/UNTS/Volume%201125/volume-1125-I-17512-English.pdf.
9. Eric Talbot Jensen, "Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?" *American University International Law Review* 18, no. 5 (2003): 1186.
10. *2011 Department of Defense Strategy for Operating in Cyberspace* (Washington: DoD, July 2011), 3.
11. Many commentators use the terms *attribution or direct responsibility*, and *imputed or indirect responsibility*. However, since *imputed responsibility* is functionally the equivalent of attributing the hostile act to the state, the term *indirect attribution* is used to clarify the discussion.
12. Jan Arno Hessbruegge, "The Historical Development of the Doctrines of Attribution and Due Diligence in International Law," *New York University Journal of International Law and Politics* 36 (Winter/Spring 2004): 268.

13. Tsagourias, "Cyber Attacks," 7.

14. Susan W. Brenner, " 'At Light Speed': Attribution and Response to Cybercrime/Terrorism /Warfare," *Journal of Criminal Law & Criminology* 97, no. 2 (2007): 379, using the terms *attack* and *attacker* attribution, or *who* and *what* attribution.

15. A *ping* is a test to see if a system on the Internet is working. *Pinging* a server tests and records the response time of the server. http://www.techterms.com/definition/ping.

16. Carr, *Inside Cyber Warfare*, 58.

17. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington: White House, May 2011), 10.

18. *Charter of the United Nations*, art. 51.

19. Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1999): 914–15.

20. For an excellent example of an application of the Schmitt analysis see Andrew C. Fultz, "Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force' Debate," *Joint Force Quarterly* 67 (4th Quarter 2012): 40–48.

21. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (as amended through 15 August 2012), 237.

22. William A. Owens et al., eds., *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington: National Academies Press, 2009), 13, http://www.nap.edu/catalog.php?record_id=12651.

23. JP 1-02, *Department of Defense Dictionary*, 2.

24. Owens et al., *Technology, Policy, Law and Ethics*, 134.

25. Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," *Harvard Journal of Law and Technology* 25, no. 2 (Spring 2012): 420–21.

26. Gen Keith B. Alexander, "Statement before the Senate Committee on Armed Services, 27 March 2012," 12–13, http://www.armed-services.senate.gov/statemnt/2012/03%20March /Alexander%2003-27-12.pdf.

27. Dr. David A. Wheeler, "Planning for the Future of Cyber Attack Attribution," statement before the US House of Representatives Committee on Science and Technology Subcommittee on Technology and Innovation, 15 July 2010, 3, http://science.house.gov/sites /republicans.science.house.gov/files/documents/hearings/071510_Wheeler.pdf.

28. Secretary of Defense Leon E. Panetta, remarks to the Business Executives for National Security, New York City, 11 October 2012, http://www.defense.gov/transcripts/transcript .aspx?transcriptid=5136.

29. *Black's Law Dictionary*, 5th ed. (St. Paul, MN: West Group, 1979), 147.

30. Scott Charney, "Rethinking the Cyber Threat: A Framework and Path Forward," Microsoft white paper (Redmond, WA: Microsoft Corp., 2009), 9.

31. Gen Keith Alexander, "U.S. Cybersecurity Policy and the Role of U.S. Cybercom," address to the Center for Strategic and International Studies, Washington, DC, 3 June 2010.

32. *US CERT Quarterly Trends and Analysis Report* 4, no. 2 (16 June 2009): 2.

33. *International Strategy for Cyberspace*, 11.

34. "China Stonewalls Panetta on Cyber Attacks," *CBS News*, 20 September 2012, http:// www.cbsnews.com/8301-202_162-57516541/china-stonewalls-panetta-on-cyberattacks/.

35. "Office of the Coordinator for Cyber Issues," http://www.state.gov/s/cyberissues/index.htm#.

36. Tsagourias, "Cyber Attacks," 7.

37. Kesan and Hayes, "Mitigative Counterstriking," 421.

38. Carr, *Inside Cyber Warfare*, 72.

39. *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization and Protection*, 17 December 2003, para. 12, http://www.dhs.gov/homeland-security-presidential-directive-7#1.

40. Ibid., para. 16.

41. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington: DHS, February 2010), 54.

42. *International Strategy for Cyberspace*, 13–14.

43. Alexander, "Statement before the Senate Committee on Armed Services," 13.

44. Charles J. Dunlap Jr., "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 93–94.